UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/068,280	02/04/2002	Mark J. McArdle	01.239.01	9739

7590 07/28/2005

ZILKA-KOTAB PC
PO Box 721120
San Jose, CA 95172-1120

EXAMINER	
HA, LEYNNA A	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 07/28/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/068,280	MCARDLE ET AL.	
	Examiner	Art Unit	
	LEYNNA T. HA	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-47 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-47 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 04 February 2002 is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____.

DETAILED ACTION

1. Claims 1-47 have been examined and are pending.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1-47 are rejected under 35 U.S.C. 102(e) as being anticipated by Douik, et al. (6,012,152).

As per claim 1:

A computerized method comprising:

determining an active networked application; **[col.3, lines 34-42]**

filtering a set of intrusion rules **[col.3, lines 20-22]** to create a subset of rules **[col.23, lines 57-63]** corresponding to the active networked application; and **[col.20, lines 15-22 and col.63-67]**

evaluating network traffic using the subset of rules. **[col.27, lines 28-43 and col.28, lines 41-45]**

As per claim 2: See col.37, lines 5-18; discusses detecting when the active networked application becomes inactive; and re-filtering the set of intrusion rules.

As per claim 3: See col.20, lines 53-55 and col.21, lines 1-2; discusses monitoring network connection terminations.

As per claim 4: See col.35, lines 53-55; discusses monitoring application terminations.

As per claim 5: See col.9, lines 25-30 and col.10, lines 8-9; discusses detecting when no networked application is active, and suspending the evaluating of network traffic until a networked application is active.

As per claim 6: See col.13, lines 37-43 and col.36, lines 65-67; discusses continuing the evaluating of network traffic if no networked application is active.

As per claim 7: See col.4, lines 66-67; discusses detecting when a network connection for an active application is initiated.

As per claim 8: See col.22, lines 49-50; discusses marking an intrusion rule corresponding to the active networked application.

As per claim 9: See col.14, lines 17-48 and col.23, lines 57-63; discusses extracting the subset of rules into an optimized set of rules.

As per claim 10: See col.13, lines 40-50; discusses analyzing network traffic on a port specified in the subset of rules.

As per claim 11: See col.13, lines 40-50 and col.19, lines 13-15; discusses analyzing network traffic for a protocol specified in the subset of rules.

As per claim 12: See col.21, lines 6-8 and col.33, line 43; discusses discarding network traffic that satisfies at least one of the subset of rules; and reporting an intrusion attempt.

As per claim 13: See col.18, lines 43-65; discusses the set of intrusion rules comprises signatures of known attacks.

As per claim 14: See col.6, lines 45-46 and col.23, lines 14-17; discusses the set of intrusion rules comprises heuristic rules.

As per claim 15:

discusses a computer-readable medium having executable instructions to cause a computer to perform a method comprising:

determining an active networked application; **[col.3, lines 34-42]**

filtering a set of intrusion rules **[col.3, lines 20-22]** to create a subset of rules **[col.23, lines 57-63]** corresponding to the active networked application; and**[col.20, lines 15-22 and col.63-67]**

evaluating network traffic using the subset of rules. **[col.27, lines 28-43 and col.28, lines 41-45]**

As per claim 16: See col.37, lines 5-18; discusses detecting when the active networked application becomes inactive, and re-filtering the set of intrusion rules.

As per claim 17: See col.20, lines 53-55 and col.21, lines 1-2; discusses monitoring network connection terminations.

As per claim 18: See col.35, lines 53-55; discusses the detecting comprises: monitoring application terminations.

As per claim 19: See col.9, lines 25-30 and col.10, lines 8-9; discusses detecting when no networked application is active', and
suspending the evaluating of network traffic until a network application is active.

As per claim 20: See col.13, lines 37-43 and col.36, lines 65-67; discusses continuing the evaluating of network traffic if no networked application is active.

As per claim 21: See col.4, lines 66-67; discusses detecting when an active application initiates a network connection.

As per claim 22: See col.22, lines 49-50; discusses marking an intrusion rule corresponding to the active networked applicaticm.

As per claim 23: See col.14, lines 17-48 and col.23, lines 57-63; discusses extracting the subset of rules into an optimized set of rules.

As per claim 24: See col.13, lines 40-50; discusses analyzing network traffic on a port specified in the subset of rules.

As per claim 25: See col.13, lines 40-50 and col.19, lines 13-15; discusses analyzing network traffic for a protocol specified in the subset of rules.

As per claim 26: See col.21, lines 6-8 and col.33, line 43; discusses discarding network traffic that satisfies at least one of the subset of rules; and reporting an intrusion attempt.

As per claim 27: See col.18, lines 43-65; discusses the set of intrusion rules comprises signatures of known attacks.

As per claim 28: See col.6, lines 45-46 and col.23, lines 14-17; discusses the set of intrusion rules comprises heuristic rules.

As per claim 29:

discusses a system comprising:

a processor coupled to a memory through a bus; and **[FIG.1 and col.11, lines 38-44]**

an intrusion prevention process executed from the memory by the processor to cause the processor to determine an active networked application **[col.13, lines 8-50]**, to filter a set of intrusion rules **[col.3, lines 20-22]** to

create a subset of rules **[col.23, lines 57-63]**corresponding to the active networked application, and to evaluate network traffic using the subset of rules. **[col.20, lines 15-22 and col.63-67]**

As per claim 30: See col.37, lines 5-18; discusses the intrusion prevention process further causes the processor to detect when the active networked application becomes inactive, and to re-filter the set of intrusion rules.

As per claim 31: See col., lines ; discusses the intrusion prevention process further causes the processor to monitor network connection terminations in detecting when the active networked application becomes inactive.

As per claim 32: See col., lines ; discusses the intrusion prevention process further causes the processor to monitor application terminations in detecting when the active networked application becomes inactive.

As per claim 33: See col.9, lines 25-30 and col.10, lines 8-9; discusses the intrusion prevention process further causes the processor to detect when no networked application is active, and to suspend evaluating network traffic until a network application is active.

As per claim 34: See col.13, lines 37-43 and col.36, lines 65-67; discusses the intrusion prevention process further causes the processor to further tilter the intrusion rules based on an operating system and to continue evaluating network traffic if no networked application is active.

As per claim 35: See col.4, lines 66-67; discusses the intrusion prevention process further causes the processor to detect when an active application initiates a network connection in determining an active networked application.

As per claim 36: See col.22, lines 49-50; discusses the intrusion prevention process further causes the processor to mark an intrusion rule corresponding to the active networked application in filtering the set of intrusion rules.

As per claim 37: See col.14, lines 17-48 and col.23, lines 57-63; discusses the intrusion prevention process further causes the processor to extract the subset of rules into an optimized set of rules in filtering the set of intrusion rules.

As per claim 38: See col.13, lines 40-50; discusses the intrusion prevention process further causes the processor to analyze network traffic on a port specified in the subset of rules in evaluating the network traffic.

As per claim 39: See col.13, lines 40-50 and col.19, lines 13-15; discusses the intrusion prevention process further causes the processor to analyze network traffic for a protocol specified in the subset of rules in evaluating the network traffic.

As per claim 40: See col.21, lines 6-8 and col.33, line 43; discusses the intrusion prevention process further causes the processor to discard network traffic that satisfies at least one of the subset of rules, and to report an intrusion attempt in evaluating the network traffic.

As per claim 41: See col.18, lines 43-65; discusses the set of intrusion rules comprises signatures of known attacks.

As per claim 42: See col.6, lines 45-46 and col.23, lines 14-17; discusses the set of intrusion rules comprises heuristic rules.

As per claim 43:

discusses an apparatus comprising:

means for determining when an active application becomes an active networked application; **[col.3, lines 34-42]**

means for filtering **[col.3, lines 20-22]** coupled to the means for determining to create a subset of rules **[col.23, lines 57-63]** corresponding to the active networked application from a set of intrusion rules; and**[col.20, lines 15-22 and col.63-67]**

means for evaluating coupled to the means for filtering to evaluate network traffic using the subset of rules. **[col.27, lines 28-43 and col.28, lines 41-45]**

As per claim 44: See col.37, lines 5-18; discusses the means for determining further detects when the active networked application becomes inactive and the means for filtering further re-filters the set of intrusion rules when the active networked application becomes inactive.

As per claim 45: See col.9, lines 25-30 and col.10, lines 8-9; discusses the means for determining further detects when no networked application is active

and the means for evaluating further suspends the evaluation of network traffic until the means for determining determines a networked application is active.

As per claim 46: See col.13, lines 37-43 and col.36, lines 65-67; discusses the means for filtering further filters the intrusion rules corresponding to an operating system and the means for evaluating continues the evaluation of network traffic when the means for determining determines no networked application is active.

As per claim 47: See col.21, lines 6-8 and col.33, line 43; discusses means for discarding network traffic that satisfies at least one of the subset of rules; and means for reporting an intrusion attempt.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA whose telephone number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax

phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

LHa

KIM VU
SUPERVISORY PATENT E
TECHNOLOGY CENTER